Data Protection and Privacy Policy

I. PURPOSE, SCOPE, AND REGULATORY FRAMEWORK

I.I Objective of This Policy

This Data Protection and Privacy Policy **(“Policy”)** establishes the formal framework under which **Finetras (“Company,” “we,” “our,” or “us”)** collects, processes, stores, transfers, safeguards, and retains personal data.

The Company is committed to maintaining the highest standards of confidentiality, integrity, and data security in accordance with applicable international data protection principles, financial regulatory obligations, and industry best practices.

I.II Scope of Application

This Policy applies to all personal data obtained through the Company’s website, trading platforms, mobile applications, communication systems, onboarding processes, and any other digital or operational channels (collectively, the “Platforms”).

By accessing or using the Company’s services, Clients acknowledge and consent to the practices described herein.

I.III Legal Basis for Processing

Personal data shall be processed only where one or more lawful grounds apply, including:

- Performance of contractual obligations;
- Compliance with legal and regulatory requirements;
- Legitimate business interests that do not override Client rights;
- Explicit consent, where required;
- Protection of the Company’s legal claims or defenses.

II. CATEGORIES OF PERSONAL DATA COLLECTED

II.I Identification and Verification Information

The Company collects identifying data such as full legal name, date of birth, nationality, government-issued identification numbers, and copies of official documents.

II.II Contact and Communication Details

Information including residential address, email address, phone number, and communication preferences may be obtained.

II.III Financial and Suitability Information

Clients may be required to provide employment status, income range, source of funds, net worth estimations, trading knowledge, and risk tolerance assessments.

II.IV Technical and Usage Information

Automated data collection may include IP addresses, browser type, device identifiers, session logs, location indicators (where permitted), and behavioral analytics.

II.V Transactional and Trading Records

Account balances, trade history, deposits, withdrawals, margin activity, and related financial records are collected and maintained.

III. REGULATORY COMPLIANCE AND VERIFICATION PROCEDURES

III.I Know Your Customer (KYC) and AML Compliance

To comply with regulatory obligations, Clients must submit documentation including proof of identity, proof of residence, and source-of-funds documentation.

Failure to provide satisfactory documentation may result in account suspension, service restriction, or termination.

III.II Third-Party Verification

The Company may utilize independent verification providers, compliance databases, and screening tools to validate identity and regulatory status.

IV. INFORMATION SECURITY AND SYSTEM PROTECTION

IV.I Technical Safeguards

The Company employs encryption protocols (including SSL/TLS), firewalls, intrusion detection systems, secure hosting environments, and vulnerability testing.

IV.II Organizational Controls

Access to personal data is limited through role-based authorization systems. Employees receive ongoing training regarding confidentiality obligations.

IV.III Two-Factor Authentication (2FA)

Enhanced account protection measures include two-factor authentication requiring secondary verification during login.

IV.IV Monitoring and Risk Detection

Continuous system monitoring is implemented to identify unauthorized access attempts, suspicious behavior, and potential cyber threats.

V. ACCOUNT ACCESS RESPONSIBILITY

V.I Credential Protection

Clients are solely responsible for safeguarding usernames, passwords, authentication codes, and registered communication channels.

V.II Reporting Unauthorized Access

Suspected account compromise must be reported immediately. The Company shall not be liable for losses arising from failure to protect credentials.

VI. COOKIES AND TRACKING TECHNOLOGIES

VI.I Use of Cookies

The Platforms utilize cookies and similar technologies to improve functionality, personalize user experience, analyze traffic, and enhance security.

VI.II Cookie Management

Clients may manage cookie settings via browser preferences, though disabling certain cookies may affect functionality.

VII. PURPOSES OF DATA PROCESSING

Personal data may be used for:

- Account administration;
- Regulatory reporting;
- Fraud prevention;
- Risk management;
- Transaction execution;
- Platform enhancement;
- Customer support;
- Dispute resolution;
- Marketing communications (subject to opt-out rights).

VIII. DATA ACCURACY AND CLIENT OBLIGATIONS

VIII.I Accuracy of Information

Clients must ensure that all submitted information remains accurate and current.

VIII.II Notification of Changes

Clients are required to promptly notify the Company of changes to personal information.

Failure to maintain accurate data may impact service delivery and compliance standing.

IX. DISCLOSURE AND THIRD-PARTY SHARING

IX.I Authorized Disclosures

Personal data may be shared with affiliates, payment service providers, liquidity providers, compliance vendors, auditors, legal advisors, and regulatory authorities.

IX.II Third-Party Safeguards

All third-party service providers are contractually obligated to implement appropriate data protection measures.

X. INTERNATIONAL DATA TRANSFERS

Personal data may be transferred to jurisdictions outside the Client’s country of residence. Where such transfers occur, appropriate safeguards shall be implemented to ensure lawful protection.

XI. DATA RETENTION

Personal data shall be retained only for as long as necessary to fulfill contractual, regulatory, and operational requirements. After such period, data will be securely deleted or anonymized.

XII. CLIENT RIGHTS

Subject to applicable law, Clients may:

- Request access to personal data;
- Request correction of inaccuracies;

- Request deletion (subject to legal retention requirements);
- Request restriction of processing;
- Object to certain processing;
- Withdraw consent where applicable.

Identity verification may be required before processing such requests.

XIII. MARKETING COMMUNICATIONS

Promotional communications may be issued periodically. Clients may opt out at any time, though regulatory and service-related notices will continue as necessary.

XIV. MINORS

The Company does not knowingly collect data from individuals under eighteen (18) years of age. Any such data discovered will be promptly deleted.

XV. INDEMNIFICATION

Clients agree to indemnify and hold harmless the Company and its representatives against claims, liabilities, and costs arising from misuse of the Platforms or violation of this Policy.

XVI. POLICY AMENDMENTS

The Company reserves the right to revise this Policy at its discretion. Amendments become effective upon publication. Continued use of services constitutes acceptance of the updated terms.